

On the Spectrum of Wenger Graphs

Sebastian M. Cioabă, Felix Lazebnik and Weiqiang Li *

February 17, 2014

Abstract

Let $q = p^e$, where p is a prime and $e \geq 1$ is an integer. For $m \geq 1$, let P and L be two copies of the $(m+1)$ -dimensional vector spaces over the finite field \mathbb{F}_q . Consider the bipartite graph $W_m(q)$ with partite sets P and L defined as follows: a point $(p) = (p_1, p_2, \dots, p_{m+1}) \in P$ is adjacent to a line $[l] = [l_1, l_2, \dots, l_{m+1}] \in L$ if and only if the following m equalities hold: $l_{i+1} + p_{i+1} = l_i p_1$ for $i = 1, \dots, m$. We call the graphs $W_m(q)$ Wenger graphs. In this paper, we determine all distinct eigenvalues of the adjacency matrix of $W_m(q)$ and their multiplicities. We also survey results on Wenger graphs.

1 Introduction

All graph theory notions can be found in Bollobás [2]. Let $q = p^e$, where p is a prime and $e \geq 1$ is an integer. For $m \geq 1$, let P and L be two copies of the $(m+1)$ -dimensional vector spaces over the finite field \mathbb{F}_q . We call the elements of P *points* and the elements of L *lines*. If $a \in \mathbb{F}_q^{m+1}$, then we write $(a) \in P$ and $[a] \in L$. Consider the bipartite graph $W_m(q)$ with partite sets P and L defined as follows: a point $(p) = (p_1, p_2, \dots, p_{m+1}) \in P$ is adjacent to a line $[l] = [l_1, l_2, \dots, l_{m+1}] \in L$ if and only if the following m equalities hold:

$$\begin{aligned} l_2 + p_2 &= l_1 p_1 \\ l_3 + p_3 &= l_2 p_1 \\ &\vdots \\ l_{m+1} + p_{m+1} &= l_m p_1. \end{aligned}$$

The graph $W_m(q)$ has $2q^{m+1}$ vertices, is q -regular and has q^{m+2} edges.

In [24], Wenger introduced a family of p -regular bipartite graphs $H_k(p)$ as follows. For every $k \geq 2$, and every prime p , the partite sets of $H_k(p)$ are two

*Department of Mathematical Sciences, University of Delaware, Newark, DE 19707-2553, USA.

copies of integer sequences $\{0, 1, \dots, p-1\}^k$, with vertices $a = (a_0, a_1, \dots, a_{k-1})$ and $b = (b_0, b_1, \dots, b_{k-1})$ forming an edge if

$$b_j \equiv a_j + a_{j+1}b_{k-1} \pmod{p} \text{ for all } j = 0, \dots, k-2.$$

The introduction and study of these graphs were motivated by an extremal graph theory problem of determining the largest number of edges in a graph of order n containing no cycle of length $2k$. This parameter also known as the Turán number of the cycle C_{2k} , is denoted by $\text{ex}(n, C_{2k})$. Bondy and Simonovits [3] showed that $\text{ex}(n, C_{2k}) = O(n^{1+1/k})$, $n \rightarrow \infty$. Lower bounds of magnitude $n^{1+1/k}$ were known (and still are) for $k = 2, 3, 5$ only, and the graphs $H_k(p)$, $k = 2, 3, 5$, provided new and simpler examples of such magnitude extremal graphs. For many results on $\text{ex}(n, C_{2k})$, see Verstraëte [20], Pikhurko [18] and references therein.

In [9], Lazebnik and Ustimenko, using a construction based on a certain Lie algebra, arrived at a family of bipartite graphs $H'_n(q)$, $n \geq 3$, q is a prime power, whose partite sets were two copies of \mathbb{F}_q^{n-1} , with vertices $(p) = (p_2, p_3, \dots, p_n)$ and $[l] = [l_1, l_3, \dots, l_n]$ forming an edge if

$$l_k - p_k = l_1 p_{k-1} \text{ for all } k = 3, \dots, n.$$

It is easy to see that for all $k \geq 2$ and prime p , graphs $H_k(p)$ and $H'_{k+1}(p)$ are isomorphic, and the map

$$\begin{aligned} \phi : (a_0, a_1, \dots, a_{k-1}) &\mapsto (a_{k-1}, a_{k-2}, \dots, a_0), \\ (b_0, b_1, \dots, b_{k-1}) &\mapsto [b_{k-1}, b_{k-2}, \dots, b_0], \end{aligned}$$

provides an isomorphism from $H_k(p)$ to $H'_{k+1}(p)$. Hence, graphs $H'_n(q)$ can be viewed as generalizations of graphs $H_k(p)$. It is also easy to show that graphs $H'_{m+2}(q)$ and $W_m(q)$ are isomorphic: the function

$$\begin{aligned} \psi : (p_2, p_3, \dots, p_{m+2}) &\mapsto [p_2, p_3, \dots, p_{m+2}], \\ [l_1, l_3, \dots, l_{m+2}] &\mapsto (-l_1, -l_3, \dots, -l_{m+1}), \end{aligned}$$

mapping points to lines and lines to points, is an isomorphism of $H'_{m+2}(q)$ to $W_m(q)$. Combining this isomorphism with the results in [9], we obtain that the graph $W_1(q)$ is isomorphic to an induced subgraph of the point-line incidence graph of the projective plane $PG(2, q)$, the graph $W_2(q)$ is isomorphic to an induced subgraph of the point-line incidence graph of the generalized quadrangle $Q(4, q)$, and $W_3(q)$ is a homomorphic image of an induced subgraph of the point-line incidence graph of the generalized hexagon $H(q)$.

We call the graphs $W_m(q)$ *Wenger graphs*. The representation of Wenger graphs as $W_m(q)$ graphs first appeared in Lazebnik and Viglione [11]. These authors suggested another useful representation of these graphs, where the right-hand sides of equations are represented as monomials of p_1 and l_1 only, see [21]. For this, define a bipartite

graph $W'_m(q)$ with the same partite sets as $W_m(q)$, where $(p) = (p_1, p_2, \dots, p_{m+1})$ and $[l] = [l_1, l_2, \dots, l_{m+1}]$ are adjacent if

$$l_k + p_k = l_1 p_1^{k-1} \text{ for all } k = 2, \dots, m+1. \quad (1)$$

The map

$$\begin{aligned} \omega : (p) &\mapsto (p_1, p_2, p'_3, \dots, p'_{m+1}), \text{ where } p'_k = p_k + \sum_{i=2}^{k-1} p_i p_1^{k-i}, \quad k = 3, \dots, m+1, \\ [l] &\mapsto [l_1, l_2, \dots, l_{m+1}], \end{aligned}$$

defines an isomorphism from $W_m(q)$ and $W'_m(q)$.

It was shown in [9] that the automorphism group of $W_m(q)$ acts transitively on each of P and L , and on the set of edges of $W_m(q)$. In other words, the graphs $W_m(q)$ are point-, line-, and edge-transitive. A more detailed study, see [11], also showed that $W_1(q)$ is vertex-transitive for all q , and that $W_2(q)$ is vertex-transitive for even q . For all $m \geq 3$ and $q \geq 3$, and for $m = 2$ and all odd q , the graphs $W_m(q)$ are not vertex-transitive. Another result of [11] is that $W_m(q)$ is connected when $1 \leq m \leq q-1$, and disconnected when $m \geq q$, in which case it has q^{m-q+1} components, each isomorphic to $W_{q-1}(q)$. In [22], Viglione proved that when $1 \leq m \leq q-1$, the diameter of $W_m(q)$ is $2m+2$. We wish to note that the statement about the number of components of $W_m(q)$ becomes apparent from the representation (1). Indeed, as $l_1 p_1^i = l_1 p_1^{i+q-1}$, all points and lines in a component have the property that their coordinates i and j , where $i \equiv j \pmod{q-1}$, are equal. Hence, points (p) , having $p_1 = \dots = p_q = 0$, and at least one distinct coordinate p_i , $q+1 \leq i \leq m+1$, belong to different components. This shows that the number of components is at least q^{m-q+1} . As $W_{q-1}(q)$ is connected and $W_m(q)$ is edge-transitive, all components are isomorphic to $W_{q-1}(q)$. Hence, there are exactly q^{m-q+1} of them. A result of Watkins [23], and the edge-transitivity of $W_m(q)$ imply that the vertex connectivity (and consequently the edge connectivity) of $W_m(q)$ equals the degree of regularity q , for any $1 \leq m \leq q-1$.

Shao, He and Shan [19] proved that in $W_m(q)$, $q = p^e$, p prime, for $m \geq 2$, for any integer $l \neq 5$, $4 \leq l \leq 2p$ and any vertex v , there is a cycle of length $2l$ passing through the vertex v . We wish to remark that the edge-transitivity of $W_m(q)$ implies the existence of a $2l$ cycle through any edge, a stronger statement. Li and Lih [12] used the Wenger graphs to determine the asymptotic behavior of the Ramsey number $r_n(C_{2k}) = \Theta(n^{k/(k-1)})$ when $k \in \{2, 3, 5\}$ and $n \rightarrow \infty$; the Ramsey number $r_n(G)$ equals the minimum integer N such that in any edge-coloring of the complete graph K_N with n colors, there is a monochromatic G . Representation (1) points to a relation of Wenger graphs with the moment curve $t \mapsto (1, t, t^2, t^3, \dots, t^m)$, and, hence, with the Vandermonde's determinant, which was explicitly used in [24]. This is also in the background of some geometric constructions by Mellinger and Mubayi [16] of magnitude extremal graphs without short even cycles.

In Section 2, we determine the spectrum of the graphs $W_m(q)$, defined as the multiset of the eigenvalues of the adjacency matrix of $W_m(q)$. Futorny and Ustimenko [6] considered applications of Wenger graphs in cryptography and coding theory, as well as some generalizations. They also conjectured that the second largest eigenvalue λ_2 of the adjacency matrix of Wenger graphs $W_m(q)$ is bounded from above by $2\sqrt{q}$. The results of this paper confirm the conjecture for $m = 1$ and 2, or $m = 3$ and $q \geq 4$, and refute it in other cases. We wish to point out that for $m = 1$ and 2, or $m = 3$ and $q \geq 4$, the upper bound $2\sqrt{q}$ also follows from the known values of λ_2 for the point-line $(q + 1)$ -regular incidence graphs of the generalized polygons $PG(2, q)$, $Q(4, q)$ and $H(q)$ and eigenvalue interlacing (see Brouwer, Cohen and Neumaier [4]). In [13], Li, Lu and Wang showed that the graphs $W_m(q)$, $m = 1, 2$, are Ramanujan, by computing the eigenvalues of another family of graph described by systems of linear equations in [10], $D(k, q)$, for $k = 2, 3$. Their result follows from the fact that $W_1(q) \simeq D(2, q)$, and $W_2(q) \simeq D(3, q)$. For more on Ramanujan graphs, see Lubotzky, Phillips and Sarnak [15], or Murty [17]. Our results also imply that for fixed m and large q , the Wenger graph $W_m(q)$ are expanders. For more details on expanders and their applications, see Hoory, Linial and Wigderson [7], and references therein.

2 Main Results

Theorem 2.1. *For all prime power q and $1 \leq m \leq q - 1$, the distinct eigenvalues of $W_m(q)$ are*

$$\pm q, \pm\sqrt{mq}, \pm\sqrt{(m-1)q}, \dots, \pm\sqrt{2q}, \pm\sqrt{q}, 0. \quad (2)$$

The multiplicity of the eigenvalue $\pm\sqrt{iq}$ of $W_m(q)$, $0 \leq i \leq m$, is

$$(q-1) \binom{q}{i} \sum_{d=i}^m \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}. \quad (3)$$

Proof. As the graph $W_m(q)$ is bipartite with partitions L and P , we can arrange the rows and the columns of an adjacency matrix A of $W_m(q)$ such that A has the following form:

$$A = \begin{matrix} & \begin{matrix} L & P \end{matrix} \\ \begin{matrix} L \\ P \end{matrix} & \begin{pmatrix} 0 & N^T \\ N & 0 \end{pmatrix} \end{matrix} \quad (4)$$

which implies that

$$A^2 = \begin{pmatrix} N^T N & 0 \\ 0 & N N^T \end{pmatrix}. \quad (5)$$

As the matrices $N^T N$ and $N N^T$ have the same spectrum, we just need to compute the spectrum for one of these matrices. To determine the spectrum of $N^T N$, let H

denote the point-graph of $W_m(q)$ on L . This means that the vertex set of H is L , and two distinct lines $[l]$ and $[l']$ of $W_m(q)$ are adjacent in H if there exists a point $(p) \in P$, such that $[l] \sim (p) \sim [l']$ in $W_m(q)$. More precisely, $[l]$ and $[l']$ are adjacent in H , if there exists $p_1 \in \mathbb{F}_q$ such that for all $i = 1, \dots, m$, we have

$$\begin{aligned} l_1 \neq l'_1 \text{ and } l_{i+1} - l'_{i+1} &= p_1(l_i - l'_i) \iff \\ l_1 \neq l'_1 \text{ and } l_{i+1} - l'_{i+1} &= p_1^i(l_1 - l'_1). \end{aligned}$$

This implies that H is actually the Cayley graph of the additive group of the vector space \mathbb{F}_q^{m+1} with a generating set

$$S = \{(t, tu, \dots, tu^m) \mid t \in \mathbb{F}_q^*, u \in \mathbb{F}_q\}. \quad (6)$$

Let ω be a complex p -th root of unity. For $x \in \mathbb{F}_q$, the trace of x is defined as $tr(x) = \sum_{i=0}^{e-1} x^{p^i}$. The eigenvalues of H are indexed after the $(m+1)$ -tuples $(w_1, \dots, w_{m+1}) \in \mathbb{F}_q^{m+1}$, and can be represented in the following form (see Babai [1] and Lovasz [14] for more details):

$$\begin{aligned} \lambda_{(w_1, \dots, w_{m+1})} &= \sum_{(t, tu, \dots, tu^m) \in S} \omega^{tr(tw_1)} \cdot \omega^{tr(tuw_2)} \cdot \dots \cdot \omega^{tr(tu^m w_{m+1})} \\ &= \sum_{t \in \mathbb{F}_q^*, u \in \mathbb{F}_q} \omega^{tr(tw_1 + tuw_2 + \dots + tu^m w_{m+1})} \\ &= \sum_{t \in \mathbb{F}_q^*, u \in \mathbb{F}_q} \omega^{tr(t(f(u)))} \quad (\text{where } f(u) := w_1 + w_2 u + \dots + w_{m+1} u^m) \\ &= \sum_{t \in \mathbb{F}_q^*, f(u)=0} \omega^{tr(t(f(u)))} + \sum_{t \in \mathbb{F}_q^*, f(u) \neq 0} \omega^{tr(t(f(u)))}. \end{aligned}$$

As $\sum_{t \in \mathbb{F}_q^*} \omega^{tr(tx)} = q-1$ for $x = 0$, and $\sum_{t \in \mathbb{F}_q^*} \omega^{tr(tx)} = -1$ for every $x \in \mathbb{F}_q^*$, we obtain that

$$\lambda_{(w_1, \dots, w_{m+1})} = |\{u \in \mathbb{F}_q \mid f(u) = 0\}|(q-1) - |\{u \in \mathbb{F}_q \mid f(u) \neq 0\}|. \quad (7)$$

Let B be the adjacency matrix of H . Then $N^T N = B + qI$; this fact can be seen easily by examining the on- and off-diagonal entries of both sides of the equation. Therefore, the eigenvalues of $W_m(q)$ can be written in the form

$$\pm \sqrt{\lambda_{(w_1, \dots, w_{m+1})} + q},$$

where $(w_1, \dots, w_{m+1}) \in \mathbb{F}_q^{m+1}$. Let $f(X) = w_1 + w_2 X + \dots + w_{m+1} X^m \in \mathbb{F}_q[X]$. We consider two cases.

1. $f = 0$. In this case, $|\{u \in \mathbb{F}_q \mid f(u) = 0\}| = q$, and $\lambda_{(w_1, \dots, w_{m+1})} = q(q-1)$. Thus, $W_m(q)$ has $\pm q$ as its eigenvalues.

2. $f \neq 0$. In this case, let $i = |\{u \in \mathbb{F}_q \mid f(u) = 0\}| \leq m$ as $1 \leq m \leq q - 1$. This shows that $\lambda_{(w_1, \dots, w_{m+1})} = i(q - 1) - (q - i) = iq - q$ and implies that $\pm\sqrt{\lambda_{(w_1, \dots, w_{m+1})} + q} = \pm\sqrt{iq}$ are eigenvalues of $W_m(q)$. Note that for any $0 \leq i \leq m$, there exists a polynomial f over \mathbb{F}_q of degree at most $m \leq q - 1$, which has exactly i distinct roots in \mathbb{F}_q . For such f , $|\{u \in \mathbb{F}_q \mid f(u) = 0\}| = i$, and, hence, there exists $(w_1, \dots, w_{m+1}) \in \mathbb{F}_q^{m+1}$, such that $\lambda_{(w_1, \dots, w_{m+1})} = iq - q$. Thus, $W_m(q)$ has $\pm\sqrt{iq}$ as its eigenvalues, for any $0 \leq i \leq m$, and the first statement of the theorem is proven.

The arguments above imply that the multiplicity of the eigenvalue $\pm\sqrt{iq}$ of $W_m(q)$ equals the number of polynomials of degree at most m (not necessarily monic) having exactly i distinct roots in \mathbb{F}_q . To calculate these multiplicities, we need the following lemma. Particular cases of the lemma were considered in Zsigmondy [25], and in Cohen [5]. The complete result appears in A. Knopfmacher and J. Knopfmacher [8].

Lemma 2.2 ([8]). *Let q be a prime power, and let d and i be integers such that $0 \leq i \leq d \leq q - 1$. Then the number $b(q, d, i)$ of monic polynomials in $\mathbb{F}_q[X]$ of degree d , having exactly i distinct roots in \mathbb{F}_q is given by*

$$b(q, d, i) = \binom{q}{i} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}. \quad (8)$$

By Lemma 2.2, the number of polynomials of degree at most m in $\mathbb{F}_q[X]$ (not necessarily monic) having exactly i distinct roots in \mathbb{F}_q is

$$\sum_{d=i}^m (q-1) b(q, d, i) = (q-1) \binom{q}{i} \sum_{d=i}^m \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}. \quad (9)$$

This concludes the proof the theorem. \square

The previous result shows that $W_m(q)$ is connected and has $2m + 3$ distinct eigenvalues, for any $1 \leq m \leq q - 1$. As the diameter of a graph is strictly less than the number of distinct eigenvalues (see [4, Section 4.1] for example), this implies that the diameter of Wenger graph is less or equal to $2m + 2$. This is actually the exact value of the diameter of the Wenger graph as shown by Viglione [22].

Since the sum of multiplicities of all eigenvalues of the graph $W_m(q)$ is equal to its order, and remembering that the multiplicity of $\pm q$ is one when $1 \leq m \leq q - 1$, we have a combinatorial proof of the following identity.

Corollary 2.3. *For every prime power q , and every m , $1 \leq m \leq q - 1$,*

$$\sum_{i=0}^m \binom{q}{i} \sum_{d=i}^m \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k} = \frac{q^{m+1} - 1}{q - 1}. \quad (10)$$

The identity (10) seems to hold for all integers $q \geq 3$, so a direct proof is desirable. Other identities can be obtained by taking the higher moments of the eigenvalues of $W_m(q)$.

As we discussed in the introduction, for $m \geq q$, the graph $W_m(q)$ has q^{m-q+1} components, each isomorphic to $W_{q-1}(q)$. This, together with Theorem 2.1, immediately implies the following.

Proposition 2.4. *For $m \geq q$, the distinct eigenvalues of $W_m(q)$ are*

$$\pm q, \pm\sqrt{(q-1)q}, \pm\sqrt{(q-2)q}, \dots, \pm\sqrt{2q}, \pm\sqrt{q}, 0,$$

and the multiplicity of the eigenvalue $\pm\sqrt{iq}$, $0 \leq i \leq q-1$, is

$$(q-1)q^{m+1-q} \binom{q}{i} \sum_{d=i}^q \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k}.$$

3 Open Questions

There are several open questions about the Wenger graphs $W_m(q)$ that we think are worth investigating: deciding whether these graphs are Hamiltonian, finding the lengths of all their cycles, determining their automorphism group, or determining the parameters of the linear codes whose Tanner graphs are the Wenger graphs.

Acknowledgments

The research of S.M. Cioabă was partially supported by National Security Agency grant H98230-13-1-0267, and the research of F. Lazebnik was partially supported by the NSF grant DMS-1106938-002.

References

- [1] L. Babai, Spectra of Cayley graphs, *J. Combin. Theory Ser. B* **27** (1979), 180–189.
- [2] B. Bollobás, *Modern Graph Theory*, Springer-Verlag New York Inc., 1998.
- [3] J. A. Bondy and M. Simonovits, Cycles of even length in graphs, *J. Combin. Theory Ser. B* **16** (1974), 97–105.
- [4] A. Brouwer, A. Cohen and A. Neumaier, *Distance-Regular Graphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1989.

- [5] S. D. Cohen, The values of a polynomial over a finite field, *Glasgow Math. J.* **14** (1973), 205–208.
- [6] V. Futorny and V. Ustimenko, On small world semiplanes with generalized Schubert cells, *Acta Appl. Math.* **98** (2007), 47–61.
- [7] S. Hoory, N. Linial and A. Wigderson, Expanders and their applications, *Bull. Amer. Math. Soc.* **43** (2006), 439–561.
- [8] A. Knopfmacher and J. Knopfmacher, Counting polynomials with a given number of zeros in a finite field, *Linear and Multilinear Algebra* **26** (1990), 287–292.
- [9] F. Lazebnik and V. Ustimenko, New examples of graphs without small cycles and of large size, *European J. Combin.* **14** (1993), 445–460.
- [10] F. Lazebnik and V. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, *Discrete Appl. Math.* **60** (1997), 275–284.
- [11] F. Lazebnik and R. Viglione, An infinite series of regular edge- but not vertex-transitive graphs. *J. Graph Theory*, **41** (2002), 249–258.
- [12] Y. Li and K.-W. Lih, Multi-color Ramsey numbers of even cycles, *European J. Combin.* **30** (2009), 114–118.
- [13] W.-C. W. Li, M. Lu and C. Wang, Recent developments in low-density parity-check codes. Coding and cryptology, 107–123, *Lecture Notes in Comput. Sci.*, 5557, Springer, Berlin, 2009.
- [14] L. Lovász, Spectra of graphs with transitive groups, *Period. Math. Hungar.* **6** (1975), 191–195.
- [15] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (3) (1988), 261–277.
- [16] K. Mellinger and D. Mubayi, Constructions of bipartite graphs from finite geometries, *J. Graph Theory* **49** (2005), no. 1, 1–10.
- [17] M.R. Murty, Ramanujan graphs, *J. Ramanujan Mat. Soc.* **23** (2003), 33–52.
- [18] O. Pikhurko, A note on the Turán function of even cycles, *Proc. Amer. Math. Soc.* **140** (2012), 3687–3992.
- [19] J.-Y. Shao, C.-X. He and H.-Y. Shan, The existence of even cycles with specific lengths in Wenger’s graph, *Acta Math. Appl. Sin. Engl.* **24** (2008), 281–288.
- [20] J. Verstraëte, On arithmetic progressions of cycle lengths in graphs, *Combin. Probab. Computing* **9** (2000), 369–373.

- [21] R. Viglione, Properties of some algebraically defined graphs, Ph.D. Thesis, University of Delaware, 2002.
- [22] R. Viglione, On the diameter of Wenger graphs, *Acta Appl. Math.* **104** (2008), 173–176.
- [23] M.E. Watkins, Connectivity of Transitive Graphs, *J. Combin. Theory*, **8**, 23–29 (1970).
- [24] R. Wenger, Extremal graphs with no C^4 's, C^6 's, or C^{10} 's, *J. Combin. Theory Ser. B* **52** (1991), no. 1, 113–116.
- [25] K. Zsigmondy, Über die Anzahl derjenigen ganzen ganzzahligen Funktionen n^{ten} Grades von x welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen, *Sitzungsher. Wien* 103 (1894), 135–144, Abt. 11.